REMARKS

Claims 1 and 29-144 are pending in the instant application. Claim 1 is rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to point out and particularly claim the subject matter which Applicants regard as their invention. Claims 1, 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,289,323 B1 (Gordon et al.)(hereinafter, "Gordon"). Claims 38 and 52 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of U.S. Patent No. 5,337,358 A)(Axelrod et al.)(hereinafter, "Axelrod"). Claims 65-71, 86-91 and 128-132 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. In addition to the foregoing rejections, the claims and the specification are objected to for informalities.

Claim 1 has been canceled and the informalities made moot. Claim 136 has been amended to correct a typographical error and claims 141-144 have been amended in order to be consistent with the new claim numbering. All other objections and rejections have been addressed herein. Therefore, Applicants respectfully submit that claims 29-144 are patentable over the cited art, for at least the following reasons.

I. Claim Objections

The Examiner has objected to the use of the term "first" in claim 1. As that claim has been canceled, the Examiner's rejection has been rendered moot.

Claims 29-144 are also objected to for using the term "critical," which the Examiner states is a term with relative meaning and thus possible of creating ambiguity. Applicants respectfully traverse this objection, since they have set forth a clear meaning to the phrase "critical document data" throughout the subject application (*see, e.g., 09/707,433 Application*, pp. 16-17). Therefore, no ambiguity may arise from the use of this terminology, and Applicants respectfully request that the Examiner withdraw this objection.

The Examiner also objects to the form of claims 136 and 137, the latter appearing to be a continuation of the former. Claim 137 has been corrected herein, and therefore this objection has been rendered moot.

II. Claim Rejection - 35 U.S.C. §112

Claim 1 is rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to point out and particularly claim the subject matter which Applicants regard as their invention. As claim 1 has been canceled herein, this rejection is rendered moot.

III. Claim Rejection - 35 U.S.C. §102(e)

Claims 1, 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gordon. Applicants respectfully traverse this rejection for at least the reasons set forth below.[1]

A. Gordon

Gordon discloses a method and apparatus for secure goods and services transactions via the postal service using an authenticated payment scheme. In the disclosed embodiment, a person or entity having an account with a postal authority issues a value message 14 in exchange for goods or services through a Payer Postal Security Device (PSD) 12. (*Gordon*, Col. 3, lines 12-15). The merchant exchanging the goods or services for the value message endorses the message with another PSD 16, and the endorsed value message 17 is then presented to the postal authority 10 for authentication. (*Id.*, lines 17-21). If the message is authenticated, the Payer PSD 12 is debited, and the payee PSD 16 is credited. (*See, id.* lines 22-24).

The value message 14 includes both text fields and encoded graphics such as one- or two-dimensional barcodes. The text fields include an algorithm ID 32, which identifies the type of cryptographic transformation algorithm used to render the Payer digital signature 50, a PSD certificate serial number 34, a Payee ID 46, and a Payer digital signature 50. (*Id at* Figure 2 and Cols. 6-7). PSD certificate serial number 34 identifies the serial number for that certificate used to authenticate the public/private key combination issued to the Payer PSD 12 by a Certificate Authority. It enables the postal authority 10 to select from a public key database, the public key that corresponds to the private key used by the Payer PSD 12 to create the digital signature 50 for the value message 14. (Thus, the Payer PSD 12 need not include the public key with the value message 14.) (*Id.*, Col 6, lines 45-51). Payer digital signature 50 is a hashed, cryptographically transformed representation of all the data fields in value message 14. (*Id.*, Col 8, lines 6-10). The

[1] Neither Gordon nor Axelrod not teach many of the limitations set forth in the dependent claims, but they are too numerous to mention. Given that neither teaches the invention set forth in the independent claims, Applicants will not address these missing limitations herein. However, by doing so, Applicants reserve their rights to address these missing limitations at a later time, if necessary.

Payer PSD 12 digitally signs these data fields using Payer's private key based on public/private key cryptography. (*Id. at* Col. 4, lines 24-40).

Once a payer issues the value message 14 to the merchant, the merchant endorses the value message 14 using a Payee PSD 16, which results in an endorsed value message 17. During the endorsement process the merchant adds additional data and fields, including an algorithm ID 52, provided in barcode form only, to identify the type of cryptographic algorithm used to render the Payee digital signature and a Payee digital signature 54 (discussed below) which is also rendered in graphical barcode format on the endorsed value message 17. (*Id.*, lines 55-60).

The Payee digital signature 54 is based upon all of the data fields contained in the endorsed value message 17. As with the Payer digital signature 50, Payee digital signature 54 is also based on public/private key cryptography, but Payee digital signature 54 uses the Payee's private key. (*Id.*, lines 44-52; Col 8, lines 29-32).

B. Applicants' Claimed Invention

Referring to the subject application, Applicants' invention as set forth in independent claims 29, 43, 75, 93, 100 comprises at least a first digital signature including a first digest of the critical document data, a second digital signature including a second digest of the critical document data and a personal identification number (PIN), and, a public key certificate including an authentic public key for validating the first and second digital signatures, wherein the first digital signature, the second digital signature, and the public key certificate are stored on the self-authenticating document. Thus, it will be appreciated that as the public key certificate that is stored on the document includes the authentic public key, the public key is also stored on the self-authenticating document. As set forth in the subject application, these latter features are critical aspects of Applicants' invention, for although public/key private key encryption can provide one level of security, verifying a digital signature using a public key of unknown origin does not necessarily prove origin or data integrity. For example, an attacker could alter a message after it is created, discard the original digital signature, and then issue a digital signature for the altered message using his own private key. He could then claim the public key that verifies the altered message's signature belongs to a third party. Thus the attacked could fraudulently attribute responsibility for an altered message to that third party. (*Serial. No., 09/707,433*, p. 13, lines 1-15)

C. **Rejection of Claims 29-64, 72-85, 92 and 100-108**

1. Public/Private Key Pair. Gordon does not anticipate claims 29-64, 72-85, 92 and 100-108 for at least two reasons. First, as will be appreciated from the subject application, the first and second digital signatures of Applicants' claimed invention are created using the identical public/private key pair (*Id.* at p. 18, lines 13-16). (The difference between the two digital signatures of Applicants' application is that with the first, an encryption algorithm is applied only to "*critical document data*," while in the second, it is applied to the "*authenticatable data string*" (or, "*critical document data*" + PIN)). Thus:

> *29. A self-authenticating document having critical document data, comprising:*
> *a first digital signature...*
> *a second digital signature...*
> *a public key certificate including an authentic public key for validating said first and second digital signatures wherein said first digital signature, said second digital signature, and said public key certificate are stored on said self-authenticating document. (Emphasis added)*

As will be appreciated from this claim, that the same public key is used to validate both the first and second digital signatures, necessitates that the same private key be used to create them in accordance with the well-known principles of public/private key cryptography.

Conversely, as discussed above, Gordon's invention necessitates that ***distinct*** and ***separate*** public/private key pairs be used; one for the Payer (in order to create Payer digital signature 50), and another for the Payee (in order to create Payee digital signature 54).

In addition, Gordon ***teaches away*** from Applicants' invention because, given the purpose of the two digital signatures in Gordon – ability to authenticate both Payer and Payee – one would not look to Gordon for the teaching of applying the same public/private key pair.

For these reasons alone, claim 29 is not anticipated by Gordon, and therefore patentable thereover. As claim 75 is substantially similar to claim 29, and claims 30-64, 72-74, 76-85, and 92 are dependent directly or indirectly from these claims, they too are patentable over Gordon.

Claim 100 is a method claim substantially similar to claims 29 and 75, and therefore Applicants reassert the foregoing arguments against it. Claims 101-108 depend directly or indirectly from claim 100, and they too are therefore patentable over Gordon.

2. Public Key Certificate, Including Public Key Stored on Document. In addition to the above stated reason, claims 29-64, 72-85, 92 and 100-108 are patentable over Gordon because, unlike Applicants' invention, where the public key certificate, including the authentic public key, is stored on the self-authenticating document, the public key of both Payer and Payee is obtained via a public "keyring."

As stated above, Gordon teaches that the postal authority 10 selects a public key from a public key database maintained by the postal authority 10:

For Payer:

PSD certificate serial number 34 enables the postal authority 10 to select a public key from a public key database maintained by the postal authority 10. The public key corresponds to a private key used by the Payer PSD 12 to create a digital signature for the value message 14. [Gordon, Col. 6, lines 45-54]

For Payee:

The payee digital signature 54 is cryptographically transformed by means of a public key stored at the postal authority 10 and accessed based upon the payee identification 46 [Id., Col. 8, lines 29-34].

In addition, not only does Gordon not teach this limitation, but it also ***teaches away*** from Applicants' invention of storing the public key certificate, including the authentic public key, on the self-authenticating document, for it clearly states that by allowing the public key to be stored in a public key database maintained by the postal authority, "*the Payer PSD 12 need not include the public key with the value message 14.*" (*Id.*, Col. 6, lines 53-54).

Axelrod, which is cited by the Examiner merely for providing support of the PDF 417 bar code format, does not provide the missing teaching.

For these additional reasons, Gordon does not anticipate claims 29-64, 72-85, 92 and 100-108 of Applicants' application under 35 U.S.C §102(e), and these claims are patentable thereover.

D. Rejection of Claims 93-99

Independent claim 93 teaches only one digital signature stored on Applicants' self-authenticating document. However, again, Gordon does not teach storing the public key certificate, including the authentic public key on the self-authenticating document, instead making the public key of both Payer and Payee obtainable via a public "keyring." Thus,

Applicants traverse the rejection of claim 93 for the same reasons as set forth in C.2 above, and submit that claim 93 is therefore patentable over Gordon. As claims 94-99 depend directly or indirectly from this claim, they too are patentable over Gordon.

E. Rejection of Claims 109-118

Independent claim 109 is a method claim that encompasses similar limitations to claims 29-64, 72-85, 92 and 100-108 above. Thus, Applicants traverse the rejection of claim 109 for the same reasons as set forth in C.1 and C.2 above, and submit that claim 109 is therefore patentable over Gordon. As claims 110-118 depend directly or indirectly from claim 109, they too are patentable over Gordon.

In addition to the foregoing reasons, Gordon also does not teach any of the following limitations:

> *determining whether said second digital signature is to be affixed to said self-authenticating document;*
> *determining whether said first digital signature is to be affixed to said self-authenticating document;*
> *affixing said public key certificate and at least one of said first digital signature and said second digital signature to said self-authenticating document in machine-readable code, based on the results of the second digital signature and first digital signature determining steps.*

In fact, Gordon ***teaches away*** from the first two steps, since it is necessary that his invention have both digital signatures present in order to render the invention operative (i.e., if the postal authority 10 is to authenticate both Payer and Payee, their respective digital signatures must be present).

For these additional reasons, Gordon does not anticipate claims 109-118 of Applicants' application under 35 U.S.C §102(e), and these claims are patentable thereover.

F. Rejection of Claims 119-127 and 133-134

Independent claim 119 sets forth a method of authenticating a self-authenticating document. Two of the steps set forth therein include processing machine-readable data on the document to obtain a digital signature data and a public key certificate, and then processing the public key certificate to obtain the authentic public key. Again, as with the claims discussed above, Gordon teaches nowhere that either the Payer or Payee public key is stored on the value message 14 (or 17) and, in fact, teaches away from these steps (*See, C.2., supra*).

In addition to the foregoing reasons, Gordon also does not teach any of the following limitations:

determining whether an authentic personal identification number (PIN) is available for appending to said critical document data;

wherein, if said authentic PIN is available;

appending said authentic PIN to said critical document data to create an authenticatable data string; and,

applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

The Examiner states that the Payer and Payee identification fields are equivalent to Applicants' PIN. Even assuming that this were correct, Payer and Payee identification fields are part of the value message 14. Gordon does not teach or suggest a step of determining whether either/both fields are "*available for appending to said critical document data*" nor does it teach/suggest the steps of "*appending said authentic PIN to said critical document data to create an authenticatable data string;*" and "*applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.*"

For these additional reasons, Gordon does not anticipate claim 119 of Applicants' application under 35 U.S.C §102(e), and this claim is thus patentable thereover. As claims 120-127 and 133-134 depend directly or indirectly from claim 119, they too are patentable over Gordon.

G. **Rejection of Claims 135-144**

Independent claims 135 and 139 are similar claims drawn to a system for reading a self-authenticating document. Gordon does not teach or suggest at least several elements of both these claims.

Applicants' claimed invention includes personal identification means (subsystem) "*for receiving a personal identification number (PIN) from a presenter of said self-authenticating document.*" Under the Examiner's contention, the Payer and Payee identification fields are

equivalent to Applicants' PIN. However, they are both part of value message 14, and therefore cannot be received from a presenter of self-authenticating document.

Claims 135 and 139 also set forth image scanning and processing means (subsystem) "*for reading said self-authenticating document and retrieving said machine-readable data from said self-authenticating document, and for assembling an authenticatable data string from said critical document data and said received PIN.*" Again, unlike Applicants' claimed invention, the Payer and Payee identification fields identified by the Examiner as being equivalent to Applicants' PIN are not assembled with other critical document data to form an "authenticatable data string." Instead they are merely used to identify Payer and Payee.

In addition to the above missing elements, Gordon also does not teach or suggest parsing means (subsystem) that parse "*machine readable data to obtain said digital signature data and said public key certificate,*" or validating means (subsystem) "*for certifying said public key certificate to obtain an authentic public key*" because neither the public key certificate nor the authentic public key is stored on Gordon's value message 17.

For the foregoing reasons, Gordon does not anticipate claims 135 and 139 of Applicants' application under 35 U.S.C §102(e), and these claims are thus patentable thereover. As claims 136-138 and 140-144 depend directly or indirectly from claim 135 and 139, they too are patentable over Gordon.

IV. Conclusion

In view of the foregoing amendments and for the above-stated reasons, Applicants submit that claims 29-144 are allowable over the prior art of record, and that the application is in condition for allowance. It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests prompt and favorable consideration of this amendment and reconsideration of the application on

whole. An early Notice of Allowance is also respectfully solicited. Should the Examiner believe that personal communication would expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (215) 986-5169.

Respectfully submitted,

BRUCE K. GEIST
THOMAS D. HAYOSH

BY: _____
Lise A. Rode
Attorney for Applicant
Reg. No. 37,226

Unisys Corporation
Unisys Way, M/S E8-114
Blue Bell, Pennsylvania 19424-0001

The Director for Patents is hereby authorized to charge payment to Deposit Account No. 19-3790 of any fees associated with this communication.

I hereby certify that this correspondence is being transmitted via facsimile ((703) 872-9306) to the United States Patent and Trademark Office on the date shown below.

May 16, 2005
Michele M. Dewitt